

Amendments to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1 1. (Original) An apparatus comprising:

2 at least one data bit generator to generate a first, second and third plurality of
3 data bits; and

4 a combiner function, coupled to the at least one data bit generator, including a
5 network of shuffle units, to combine the third plurality of data bits, using the first and
6 second plurality of data bits as first input data bits and control signals respectively of the
7 network of shuffle units.

1 2. (Original) The apparatus of claim 1, wherein at least one of the shuffle units

2 comprises a first and a second flip-flop to store a first and a second state value, and a
3 plurality of selectors coupled to the first and second flip-flops in a topological manner to
4 control selective output of one of the first and second state values based on a
5 corresponding one of said second plurality of data bits.

1 3. (Original) The apparatus of claim 2, wherein said plurality of selectors are

2 coupled to said first and second flip-flops of the shuffle unit in a topological manner that
3 results in the first state value of the shuffle unit being output when the corresponding
4 one of said second plurality of data bits is in a first state, and the second state value of
5 the shuffle unit being output when the corresponding one of said second plurality of data
6 bits is in a second state.

1 4. (Original) The apparatus of claim 2, wherein said plurality of the selectors are

2 further coupled to said first and second flip-flops of the shuffle unit to control selective

3 modification of the first and second state values stored in said first and second flip-flops
4 of the shuffle unit based on the same corresponding one of said second plurality of data
5 bits.

B¹ 1 5. (Original) The apparatus of claim 4, wherein said plurality of selectors are
2 coupled to said first and second flip-flops of the shuffle unit in a topological manner that
3 results in the first state value being output and the first and second flip-flops of the
4 shuffle unit to store said second state value and a second input data bit respectively
5 when the corresponding one of said second plurality of data bits is in a first state, and
6 the second state value being output and the first and second flip-flops of the shuffle unit
7 to store the second input data bit and said first state value respectively when the
8 corresponding one of said second plurality of data bits is in a second state.

1 6. (Original) The apparatus of claim 5, wherein the second input value is a selected
2 one of an output data bit of an immediately preceding shuffle unit and an output data bit
3 generated from said first plurality of data bits.

1 7. (Original) The apparatus of claim 1, wherein at least one of the shuffle units
2 comprises a first and a second flip-flop to store a first and a second state value, and a
3 plurality of selectors coupled to the first and second flip-flops to control modification of
4 the first and second state values based on a corresponding one of said second plurality
5 of data bits.

1 8. (Original) The apparatus of claim 7, wherein said plurality of selectors are
2 coupled to the first and second flip-flops in a topological manner that results in the first
3 and second flip-flops of the shuffle unit to store said second state value and a second

4 input data bit respectively when the corresponding one of said second plurality of data
5 bits is in a first state, and the first and second flip-flops of the shuffle unit to store the
6 second input data bit and said first state value respectively when the corresponding one
7 of said second plurality of data bits is in a second state.

B¹
1 9. (Original) The apparatus of claim 8, wherein the shuffle units are serially coupled
2 to each other with a first of the shuffle unit serially coupled to the first XOR gate, and
3 said second input data bit is a selected one of an output bit of an immediately preceding
4 shuffle unit and an output bit generated from the first plurality of data bits.

1 10. (Original) The apparatus of claim 1, wherein the combiner function further
2 comprises an exclusive-OR gate to combine the first plurality of data bits for the network
3 of shuffle units.

1 11. (Original) The apparatus of claim 1, wherein the combiner function further
2 comprises an exclusive-OR gate to combine the third plurality of data bits using an
3 output bit of the network of shuffle units.

1 12. (Original) The apparatus of claim 11, wherein the apparatus further comprises a
2 register coupled to the XOR gate to store a cipher key and allow the stored cipher key
3 to be periodically modified by the output of the exclusive-OR gate.

1 13. (Original) The apparatus of claim 12, wherein the apparatus further comprises a
2 function block coupled to the register to successively transform the modified cipher key,
3 and a mapping block coupled to the register to generate a pseudo random bit sequence
4 based on the successive transformed states of the modified random number.

1 14. (Original) The apparatus of claim 1, wherein the at least one data bit generator
2 comprises a plurality of LFSRs to generate said first, second, and third plurality of data
3 bits.

B¹
1 15. (Original) The apparatus of claim 1, wherein the apparatus is a stream cipher.

1 16. (Cancelled).

1 17. (Currently Amended) ~~The apparatus of claim 14,~~ An apparatus comprising:
2 a first XOR gate to receive a first plurality of data bits and combine them
3 into a second data bit;

4 a network of shuffle units, coupled to the first XOR gate, to output a third
5 data bit by shuffling and propagating the second data bit through the network of
6 shuffle units under the control of a fourth plurality of data bits; and

7 a second XOR gate coupled to the network of shuffle units to combine a
8 fifth plurality of data bits using the third data bit;

9 wherein at least one of the shuffle units comprises a first and a second flip-flop to
10 store a first and a second state value, and a plurality of selectors coupled to the first and
11 second flip-flops to control selective output of one of the first and second state values
12 based on a corresponding one of said fourth plurality of data bits.

1 18. (Currently Amended) The apparatus of claim ~~15~~7, wherein said plurality of
2 selectors are coupled to the first and second flip-flops of the shuffle unit in a topological
3 manner that results in the first state value of the shuffle unit being output when the
4 corresponding one of said fourth plurality of data bits is in a first state, and the second

5 state value of the shuffle unit being output when the corresponding one of said fourth
6 plurality of data bits is in a second state.

B) 1 19. (Currently Amended) The apparatus of claim ~~168~~168, wherein said plurality of the
2 selectors are further coupled to the first and second flip-flops to control selective
3 modification of the first and second state values stored in the first and second flip-flops
4 of the shuffle unit based on the same corresponding one of said fourth plurality of data
5 bits.

1 20. (Currently Amended) The apparatus of claim ~~179~~179, wherein said plurality of
2 selectors are coupled to the first and second flip-flops of the shuffle unit in a topological
3 manner that results in the first state value being output and the first and second flip-
4 flops of the shuffle unit to store said second state value and a sixth data bit respectively
5 when the corresponding one of said fourth plurality of data bits is in a first state, and the
6 second state value being output and the first and second flip-flops of the shuffle unit to
7 store the sixth data bit and said first state value respectively when the corresponding
8 one of said fourth plurality of data bits is in a second state.

1 21. (Currently Amended) The apparatus of claim ~~1820~~1820, wherein the shuffle units are
2 serially coupled to each other with a first of the shuffle unit serially coupled to the first
3 XOR gate, and said sixth data bit is a selected one of said second data bit and the
4 output of an immediately preceding shuffle unit.

1 22. (Currently Amended) The apparatus of claim 1~~[[4]]~~[[4]]~~7~~, wherein at least one of the
2 shuffle units comprises a first and a second flip-flop to store a first and a second state
3 value, and a plurality of selectors coupled to the first and second flip-flops to control

4 modification of the first and second state values based on a corresponding one of said
5 fourth plurality of data bits.

B¹
1 23. (Currently Amended) The apparatus of claim ~~20~~2, wherein said plurality of
2 selectors are coupled to the first and second flip-flops of the shuffle unit in a topological
3 manner that results in the first and second flip-flops of the shuffle unit to store said
4 second state value and a sixth data bit respectively when the corresponding one of said
5 fourth plurality of data bits is in a first state, and the first and second flip-flops of the
6 shuffle unit to store the sixth data bit and said first state value respectively when the
7 corresponding one of said fourth plurality of data bits is in a second state.

1 24. (Currently Amended) The apparatus of claim ~~21~~3, wherein the shuffle units are
2 serially coupled to each other with a first of the shuffle unit serially coupled to the first
3 XOR gate, and said sixth data bit is a selected one of said second data bit and the
4 output of an immediately preceding shuffle unit.

1 25. (Currently Amended) The apparatus of claim ~~1~~[[4]]7, wherein the apparatus
2 further comprises a register coupled to the second exclusive-OR gate to store a value to
3 be periodically modified using the result of said combination of the fifth plurality of data
4 bits.

1 26. (Currently Amended) The apparatus of claim ~~23~~5, wherein the apparatus further
2 comprises a function block coupled to the register to successively transform a modified
3 version of the stored value, and a mapping block coupled to register to generate a
4 pseudo random bit sequence based on the successively transformed states of the
5 modified value.

1 27. (Currently Amended) The apparatus of claim ~~142~~26, wherein the apparatus is a
2 stream cipher.

B
1 28. (Original) A method comprising:
2 generating a first, second and third plurality of data bits; and
3 shuffling and propagating a fourth data bit generated from the first plurality of
4 data bits, under the control of the second plurality of data bits, to output a fifth data bit to
5 combine the third plurality of data bits.

1 29. (Currently Amended) The method of claim ~~26~~8, wherein the fourth data bit is
2 serially shuffle and propagated, and at each stage, a first state value is output when the
3 corresponding one of said second plurality of data bits is in a first state, and a second
4 state value is output when the corresponding one of said second plurality of data bits is
5 in a second state.

1 30. (Currently Amended) The method of claim ~~26~~8, wherein the fourth data bit is
2 serially shuffle and propagated, and at each stage, a first of the state values is replaced
3 by an input value, and shuffled, when the corresponding one of said second plurality of
4 data bits is in a first state, and a second of the state values is replaced by the input
5 value, and shuffled, when the corresponding one of said second plurality of data bits is
6 in a second state.
